1

IT-Sicherheit im Strafrecht ("digitaler Hausfriedensbruch") - Der Gesetzentwurf des Bundesrates zur Einführung eines neuen § 202e StGB

von **Dr. Eren Basar**, RA und FA für Strafrecht, Compliance Officer (TÜV), Wessing & Partner Rechtsanwälte mbB, Düsseldorf

I. Hintergrund

Immer mehr gerät die Integrität und der Schutz informationstechnologischer Systeme (IT) in das Blickfeld des Strafrechts. Der „Cyberkrieg“ ist heute fast genauso präsent wie der „Terrorismus“ und immer häufiger wird beides im Zusammenhang gesehen.[1] Richtig ist, dass die Bedrohungslage für die Sicherheit der IT aufgrund von vielfältigen Angriffsmöglichkeiten heute eine andere ist als vor fünf oder zehn Jahren.[2] Nahezu täglich gibt es Meldungen über sog. „Denial of Service“ Attacken, die dazu führen, dass ganze IT-Systeme arbeitsunfähig gemacht werden.[3] Erst Ende November hat eine solche Attacke zu einer Großstörung bei der Telekom und zu einem Ausfall von 900.000 Anschlüssen geführt.[4] Der Gesetzgeber hat auf die neue Lage bereits 2015 mit dem IT-Sicherheitsgesetz reagiert und für bestimmte Unternehmen, die so genannten Betreiber kritischer Infrastrukturen, bestimmte Verhaltenspflichten eingeführt.[5] Strafrechtlich abgesichert wurden die Pflichten in diesem Gesetz nicht.[6] Vor dem Hintergrund der zunehmenden Bedrohungen für die IT-Sicherheit hat der Bundesrat am 23.09.2016 auf Antrag des Landes Hessen einen Gesetzentwurf beschlossen, der die unbefugte Nutzung von IT-Systemen als sog. „digitalen Hausfriedensbruch“ unter Strafe stellen und den strafrechtlichen Schutzbereich anpassen soll.[7] Der Bundesrat ist der Ansicht, dass die bisherigen Bemühungen[8] nicht ausreichend waren und die technischen Entwicklungen im Kernstrafrecht zu „spürbaren Strafbarkeitslücken“ führen.[9] Dieses schütze in den §§ 202a, 303a und 303b StGB nur bestimmte Daten, nicht aber technische Systeme als solche. Dies genügt dem Bundesrat für einen „wirksamen Rechtsgüterschutz“ nicht mehr.[10]

Zur weiteren Begründung des strafrechtlichen Regelungsbedarfs verweist der Gesetzesentwurf auf die Convention on Cybercrime vom 23.11.2001, die den Vertragsparteien auferlegt hatte, die unbefugte Nutzung von Computersystemen als Straftat zu umschreiben.[11] Der Gesetzgeber hatte 2007 bewusst die in der Convention vorhandene Option gewählt und § 202a StGB so ausgestaltet, dass dieser als zusätzliche Voraussetzung die Überwindung einer besonderen Zugangssicherung beinhaltet. Grund hierfür war, dass eine Überkriminalisierung befürchtet wurde.[12] Angesichts der stetig wachsenden Bedeutung der IT-Wirtschaft sieht der Bundesrat in dieser Ausgestaltung nunmehr einen Nachteil. Als weiteren „eindrucksvollen Beleg für die Lückenhaftigkeit“ des strafrechtlichen Rechtsgüterschutzes wird zudem auf eine im letzten Jahr ergangene Entscheidung des BGH hingewiesen. In dieser musste der BGH eine Verurteilung wegen § 202a StGB aufheben, weil die Überwindung der Zugangssicherung durch das Ausgangsgericht nicht festgestellt werden konnte.[13] In dem zu entscheidenden Fall hatten sich zwei Heranwachsende zusammengeschlossen, um ein „Botnetzwerk“ aufzubauen.[14] Hierzu hatten sie spezielle Schadsoftware programmiert und über ein Netzwerk, welches zum Download von Filmen und Musikdateien genutzt wurde, verbreitet. Die Schadsoftware war so programmiert, dass die Firewall umgangen und das Betriebssystem des Computers dahin gehendverändert wurde, dass jede Eingabe an den infizierten Rechnersystemen, darunter Zugangsdaten zu diversen Accounts nebst Passwörtern, an eine von den beiden Angeklagten eingerichtete Datenbank übertragen wurde. Die Entscheidung verdeutliche, so der Gesetzesentwurf, dass die §§ 202a, 303a, 303b StGB nicht tauglich seien, die Erscheinung der „Botnetzkriminalität wirkungsvoll zu bekämpfen“, da die Anforderungen an die Feststellungen, die der BGH formuliert hat, hinsichtlich des Programms zu hoch seien.[15] In Zukunft müsste man – wollte man diesen Anforderungen gerecht werden – die betroffenen Systeme durch Sachverständige untersuchen lassen. Dies würde für die Inhaber der Geräte zu „Unannehmlichkeiten“ führen, weil eine Datenspiegelung vorgenommen werden müsste, mit der Folge, dass auch „höchstpersönliche“ Daten aus dem Kernbereich privater Lebensgestaltung der Opfer ausgehändigt würden. Diese würde zu einem aus Opfersicht „Gefühl des Überwachtseins“ führen.

II. Umfang der Kriminalisierung

Eingeführt werden soll ein neuer §202e StGB-E,[16] der in Absatz 1 die (schlichte) unbefugte Zugangsverschaffung zu einem informationstechnischen System (Nr. 1) und den Gebrauch eines solchen (Nr. 2) mit bis zu einem Jahr Freiheitstra-

fe oder Geldstrafe unterstellt, wenn die Tat jeweils geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Strafbar soll außerdem sein, einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf eines informationstechnischen Systems zu beeinflussen oder in Gang zu setzen (Nr. 3). Erfasst sind somit alle denkbaren Nutzungen und Eingriffe in IT-Systeme, die ohne wirksame Einwilligung erfolgen. Dies soll für Cookies ebenso gelten wie für Applikationen (Apps), die einen größeren Funktionsumfang haben als in der Beschreibung angegeben und in der die Nutzer über Zugriffsrechte getäuscht wurden. § 202e StGB-E sieht bewusst nicht vor, dass der Tatbestand auf fremde informationstechnische Systeme begrenzt wird. Erfasst werden sollen auch Fälle, in denen der Arbeitnehmer vom Arbeitgeber ein mobiles System zur alleinigen Nutzung erhält und der Arbeitgeber dieses heimlich infiltriert.[17] Aufgrund der Weite des Tatbestandes soll der Tatbestand mit zwei Einschränkungen versehen werden: Zum einen werden die informationstechnischen Systeme in § 202e Abs. 6 Nr. 1 StGB-E derart definiert, dass nicht vernetzte elektronische Unterhaltungsgeräte, Spielzeuge oder Taschenrechner aus dem Tatbestand ausgenommen werden.[18] Des Weiteren soll die in § 202e Abs. 1 Satz 2 StGB-E verankerte Eignungsklausel Bagatellfälle ausnehmen.[19] Bedenken hinsichtlich der Bestimmtheit werden mit dem Hinweis auf die Parallele in § 201 StGB und einer Entscheidung des BVerfG zurückgewiesen.

Die Strafbarkeit wird in § 202e Abs. 2, 3 StGB-E noch erweitert. In § 202e Abs. 2 StGB-E wird der Strafrahmen auf bis zu fünf Jahre erhöht, wenn der Täter gegen Entgelt oder mit Schädigungsabsicht handelt. § 202e Abs. 3 StGB-E enthält eine weitere Erhöhung in Form eines Regelbeispiels mit einem Strafrahmen von bis zu zehn Jahren, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt (Nr. 1), den Zugang zu einer großen Anzahl von informationstechnischen Systemen verschafft, eine große Anzahl von informationstechnischen Systemen in Gebrauch nimmt, eine große Anzahl von Datenverarbeitungsvorgängen oder informationstechnischen Abläufen beeinflusst (Nr. 2) oder in der Absicht handelt, eine Gefahr für die öffentliche Sicherheit, eine gemeingefährliche Straftat oder eine besonders schwere Straftat gegen die Umwelt nach § 330 StGB herbeizuführen oder zu ermöglichen (Nr. 4). Sollte vom Täter beabsichtigt sein die Funktionsfähigkeit kritischer Infrastrukturen zu beeinträchtigen, soll die Mindeststrafe gemäß § 202e Abs. 4 StGB-E auf ein Jahr heraufgesetzt werden. Für die Definition des Begriffs „kritische Infrastruktur“ wird auf § 2 Abs. 10 BSIG und die dazu gehörige Verordnung verwiesen.[20] Des Weiteren wird in § 202e Abs. 5 StGB-E die Versuchsstrafbarkeit eingeführt. Diese sei notwendig, „um z.B. beim Einsatz nicht offen ermittelnder Polizeibeamter oder verdeckter Ermittler dennoch zu einer Strafbarkeit des Täters zu gelangen“. Für die Absätze 1 und 2 wird in § 202e Abs. 7 StGB-E schließlich eine Antragspflicht statuiert: Wenn der Verletzte ein Angehöriger, der Vormund oder der Betreuer ist oder mit dem Täter in häuslicher Gemeinschaft lebt, wird die Tat nur auf Antrag verfolgt. Für dieselben Absätze soll zudem § 374 SPO Anwendung finden. Der Bundesrat will so bei Fällen geringeren Gewichts die Staatsanwaltschaft durch den Verweis auf den Privatklageweg entlasten.

III. Gesetzeszweck und Legitimation

Grund für diese Kriminalisierung ist aus Sicht des Bundesrates die unverändert hohe Verletzungsanfälligkeit von IT-Systemen und die zunehmend massenhafte Infizierung von Rechnern mit Infiltrationssoftware.[21] In der Schadsoftware sieht der Bundesrat eine große Gefahr. Immerhin haben die Täter oftmals das Ziel, die so infiltrierten Systeme als „Bot“ zu nutzen und sämtliche Funktionen und Daten des Systems für weitere Aktivitäten – in der Regel Cyberstraftaten – zu gebrauchen. Ausführlich wird beschrieben, wie ein „Botnetzwerk“ funktioniert und welchen Schaden es anrichten kann. Ein infiziertes System könne ohne Probleme ausgespäht und ferngesteuert werden. So könnten Webcams und Mobiltelefone unbemerkt eingeschaltet werden, um heimlich Videos und Töne zu übertragen. Die Ausspähung von Smartphones könne auch Passwörter erfassen. Bedacht werden müsse, dass nahezu alle beruflichen und geschäftlichen Aktivitäten betroffen sein können.[22] Daneben wird auf die durch Botnetzwerke verursachten Schäden in Milliardenhöhe hingewiesen, die darauf zurückzuführen sind, dass Botnetzwerke regelmäßig für sog. Denial of Service Attacken (DOS) genutzt werden, die große Netzwerke deaktivieren.[23] Behauptet wird, dass das Strafrecht deswegen benötigt wird, weil der Einzelne sich gegen diese Bedrohung selbst kaum schützen kann. Dies dürfte in dieser Einseitigkeit aber kaum zu halten sein.[24] Schuldig bleibt der Entwurf zudem die Antwort darüber, warum der derzeitige Strafrechtsschutz lückenhaft sein soll. Bei genauerer Betrachtung der einzelnen Stadien des Aufbaus und Betriebs von Botnetzen wird man in den meis-

ten Konstellationen sehr wohl annehmen müssen, dass eine Strafbarkeit vorliegt.[25] Schon eine einfache Firewall kann ausreichend sein, den Schutz durch § 202a StGB zu aktivieren.[26] Der heimliche Zugriff auf (später zu nutzende) Passwörter kann zudem eine – in der Praxis meist nicht beachtete – Strafbarkeit nach den §§ 43 Abs. 2 Nr. 1, 44 BDSG nach sich ziehen.[27] Richtig ist jedoch, dass die Feststellung digitaler Zugangssicherungen unter dem Regime des Strengbeweises der StPO aufwendig sein kann. Die Ausführungen im Entwurf rund um das BGH-Urteil zeugen eher davon, dass der tatsächliche Antrieb des Entwurfs ist, mit der Strafnorm eine Vorfeldtat zum bestehenden Kanon der Cyberdelikte zu schaffen und die Beweisführung zu erleichtern.

IV. Bewertung und Ausblick

Die zunehmend zentrale Bedeutung der IT für Gesellschaft und Wirtschaft rechtfertigt es, sich Gedanken darüber zu machen, ob eine Ausweitung des strafrechtlichen Schutzes angezeigt ist. Die Strafrechtsordnung muss sich neuen gesellschaftlichen Bedrohungen stellen, um auf der Höhe der Zeit zu bleiben. Die Integrität informationstechnischer Systeme ist verfassungsrechtlich als Schutzgut anerkannt und als strafrechtliches Rechtsgut auch konkret genug, um den Einsatz des Strafrechts zu rechtfertigen. Indes wird der Entwurf den verfassungspolitischen Anforderungen an die Begründung eines neuen Straftatbestands nicht gerecht: Die Herleitung der Strafwürdigkeit ist oberflächlich und präsentiert eine alte Diskussion im neuen Gewand, mit der Behauptung, es bestehe aufgrund einer Entscheidung (über ein offensichtlich schlecht ermitteltes Verfahren) eine Lücke, wohlwissend, dass die fehlende Strafbarkeit eine auf Sachgründen fußende Entscheidung des Gesetzgebers war, die strafrechtliche Schutzzone nicht überzustrapazieren. Das Ansinnen, es den Ermittlern und Gerichten so einfach wie möglich zu machen, setzt sich in der Ausgestaltung des neuen Straftatbestandes fort. Der Straftatbestand wird extrem weit formuliert (inklusive Versuchsstrafbarkeit),[28] um alle denkbaren Fallgestaltungen zu erfassen. Allerdings geht dies so weit, dass in der gegenwärtigen Fassung jede unbefugte Nutzung eines IT-Systems den objektiven Tatbestand erfüllen kann. Ein solcher Tatbestand mag aus Sicht von Ermittlern wünschenswert sein. Das Bedürfnis, Beweiserleichterungen zu schaffen, kann in einem rechtstaatlichen Strafrecht jedoch eine Erweiterung der Strafrechtszone nicht begründen.[29]

Es ist nicht wahrscheinlich, dass dieser Entwurf Gesetz wird. Die Bundesregierung hat dem derzeitigen Entwurf jedenfalls in ihrer Stellungnahme mit einer ganzen Reihe von den o.g. Kritikpunkten eine Absage erteilt.[30] Es bleibt zu hoffen, dass es hinsichtlich dieses Entwurfs dabei bleibt. Allerdings hat die Bundesregierung auch erklärt, dass das Ziel des Gesetzesentwurfes anerkennenswert ist und eine Prüfung angekündigt, ob sie einen eigenen Entwurf vorlegt. Das Thema „IT-Sicherheit im Strafrecht“ dürfte damit nicht vom Tisch sein.[31]

---

1 Dies wird als „Cyberterrorismus“ bezeichnet. Das Bundesministerium des Innern bezeichnet hierunter eine „Form von Terrorismus, bei der das Internet als Waffe genutzt wird. Es werden also mit Hilfe von Internet-Technologien Angriffe auf Computersysteme verübt", abrufbar unter http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberterrorismus/cybersterrorismus.html, zuletzt geprüft 17.11.2016.

2 Vgl. dazu den aktuellen Bericht zur Lage der IT-Sicherheit in Deutschland des Bundesamts für Sicherheit in der Informationstechnologie (BSI), abrufbar unter https://www.bsi.bund.de/DE/Themen/CyberSicherheit/Gefaehrdungslage/Lageberichte/cs_Lageberichte_node.html, zuletzt geprüft am 17.11.2016.

3 Laut einer Studie des Digitalverbands Bitkom aus dem Jahre 2015 war jedes zweite Unternehmen schon von (internen oder externen) Angriffen auf die IT betroffen. Am prominentesten dürfte die Attacke auf die IT-Sicherheit des Deutschen Bundestages aus 2015 sein. Anfang des Jahres 2016 wurde ein Krankenhaus in Neuss Opfer eines Angriffs auf die IT. Jüngst gelang es Hackern zudem die beiden Anbieter „Twitter“ und „Spotify“ zu infiltrieren. Am 05.11.2016 wurde bekannt, dass dieselben Hacker erstmals einen ganzen Staat ins Visier (Nigeria) genommen haben.

4 Vgl. www.heise.de/newsticker/meldung/Grossstoerung-bei-der-Telekom-Schlecht-programmierte-Schadsoftware-verhinderte-schlimmere-Folgen-3506909.html, zuletzt geprüft 03.12.1016.

5 Zum Ganzen Gitter /Meißner/Spauschus, ZD 2015, 512.

6 Ob das Gesetz mittelbar, nämlich durch Statuierung von Pflichten i.S.d. § 13 StGB, ein Strafbarkeitsrisiko begründet ist bislang – soweit ersichtlich – nicht diskutiert worden. Eine solche Pflicht würde sich allerdings regelmäßig an die intern Verantwortlichen richten und nicht an die Angreifer.

7 BT-Drs. 18/10182; zum Gesetzentwurf des Landes Hessen und zum Beschluss des Bundesrates vom 23.09.2016, abrufbar unter http://kripoz.de/2016/07/06/entwurf-eines-strafrechtsaenderungsgesetzes-strafbarkeit-der-unbefugten-benutzung-informationstechnischer-systeme-digitaler-hausfriedensbruch/, zuletzt geprüft am 17.11.2016, sowie Mavany, KriPoZ 2016, 106.

8 BT-Drs. 18/10182, S. 11: Gemeint sind das 41. Strafrechtsänderungsgesetz vom 07.08.2007, der neue Straftatbestand der Datenhehlerei (§ 202d StGB) und das Gesetz zur Einführung einer Speicherpflicht vom 10.12.2015 (sog. Vorratsdatenspeicherung),

9 BT-Drs. 18/10182, S. 3.

10 Als Beispiel wird in BT-Drs. 18/10182, S. 4 ein fiktiver Fall gebildet, in dem der Täter unbemerkt beobachtet wie das Opfer den Passcode bei seinem Smartphone eingibt. Im Anschluss gelingt es dem Täter das Gerät unbemerkt an sich zu bringen und das Smartphone mit dem Passwort zu entsperren und die dortigen Daten (Bilder, geschäftliche Daten usw.) zu betrachten. Wenn der Täter das Gerät dann wieder zurücklegt, sei diese Vorgehensweise des Täters im Kernstrafrecht derzeit straflos.

11 BT-Drs. 18/10182, S. 12.

12 Die Neuerung enthielt nach Hilgendorf (in: Leipziger Komm. StGB, 12. Aufl. 2009, § 202a Rn. 3) eine Vorverlagerung des strafrechtlichen Schutzes. Inkriminiert wurde nämlich nicht mehr (nur) die Verschaffung von Daten, sondern die Verschaffung des Zugangs zu diesen. Auch bei dieser Fassung des § 202a StGB blieben hinsichtlich der Reichweite Bedenken bestehen, vgl. Walter/Kargl in: NK-StGB, 3. Aufl. 2013, § 202a Rn. 3a.

13 BT-Drs. 18/10182, S. 12, mit Verweis auf BGH, Beschl. v. 21.07.2015 - 1 StR 16/15 - NJW 2015, 3463.

14 Als solches Botnetzwerk bezeichnet der Bundesrat in seinem Gesetzesentwurf (BT-Drs. 18/10182, S. 1) eine große Anzahl von mit dem Internet ständig oder zeitweise verbundenen informationstechnischen Systemen wie Computer oder Mobiltelefone, die – von ihrem rechtmäßigen Nutzer unbemerkt – mit Schadprogrammen infiltriert sind und daher einzeln oder in ihrer Gesamtheit einer fremden Kontrolle unterliegen.

15 Die Anforderungen seien nach BT-Drs. 18/10182, S. 13 durch die Tatgerichte kaum zu erfüllen. Der BGH hatte nämlich aufgegeben, in den Urteilsgründen die Wirkweise der von dem Angeklagten bereitgestellten Software, welche die Benennung der im konkreten Einzelfall umgangenen Zugangssicherung enthalten müsse, hinreichend genau darzustellen, wofür ein pauschaler Verweis auf das Bestehen der Sicherung nicht ausreiche.

16 Im Folgenden BT-Drs. 18/10182, S. 9 und S. 13 ff.

17 Umgekehrt wäre unter der jetzigen Fassung ebenfalls denkbar, dass Arbeitnehmer sich strafbar machen, wenn sie eigene Geräte nach Absprache für den Arbeitgeber nutzen (sog. „bring your own device“ oder einfach „BYOD“), die Nutzung des eigenen Geräts im Netzwerk des Arbeitgebers aber unter Verletzung der IT-Richtlinie, also „unbefugt“, genutzt wird.

18 Im Sinne des § 202e StGB-E sind informationstechnische Systeme nur solche, die zur Verarbeitung personenbezogener Daten geeignet und bestimmt sind oder Teil einer Einrichtung oder Anlage sind, die wirtschaftlichen, öffentlichen wissenschaftlichen, künstlerischen, gemeinnützigen oder sportlichen Zwecken dient oder die den Bereichen Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Versorgung, Haustechnik oder Haushaltstechnik angehört.

19 Berechtigte Interessen können dabei materielle oder ideelle, private oder öffentliche sein, sofern sie nur als vom Recht als schutzwürdig anerkannt sind.

20 Die Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz wurde am 22.04.2016 erlassen (BGBl I 2016, 958) und definiert eine Anlage i.S.d. § 2 Abs. 10 BSIG als eine, von deren Versorgungsleistung jeweils 500.000 oder mehr Bürger abhängig sind.

21 BT-Drs. 18/10182, S. 2, 14: Täglich seien bis zu 60.000 Infektionen registriert. 40% aller internetfähigen Rechner seien betroffen.

22 BT-Drs. 18/10182, S. 2.

23 Diese sind regelmäßig nach § 303b StGB strafbar.

24 Vgl. zu den Möglichkeiten sich zu schützen www.pcwelt.de/ratgeber/Ist-der-PC-infiziert-Was-sind-Botnetze-und-was-hilft-dagegen-1084516.html, zuletzt geprüft am 17.11.2016.

25 Zum Ganzen ausführlich Mavany, KriPoZ 2016, 106, 108; zustimmend Kochheim, Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, 2015, S. 239 f. So sieht es auch die Bundesregierung in ihrer Stellungnahme zum Entwurf BT-Drs. 18/10182, S. 19.

26 Walter/Kargl in: NK-StGB, § 202a Rn. 10. Die Nutzung der heimlich erspähten Daten wird regelmäßig § 263 StGB oder § 263a StGB erfüllen.

27 Mavany, KriPoZ 2016, 106, 109.

28 Die Begründung ist nahezu ohne Substanz: Der Einsatz von heimlichen Ermittlungsmethoden sei bei Internetermittlungen von hoher praktischer Relevanz. Hier müsse man „dennoch“ zu einer Strafbarkeit der Täter kommen. Im Ergebnis wird offensichtlich darauf verwiesen, dass die Versuchsstrafbarkeit benötigt wird um die strafrechtliche Schutzzone so weit auszudehnen, dass die Vorfeldtätigkeit der Täter vor Zugang zum IT-Gerät bereits strafrechtlich sanktioniert werden kann. Substanziell soll hier Gefahrenabwehrrecht zum Straftatbestand erhoben werden.

29 Basar, Modernes Strafrecht – vergessene Freiheit?, S. 224 f.

30 BT-Drs. 18/10182, S. 19.

31 Nach der Attacke auf die Telekom wird in Wirtschaft und Politik bereits über Konsequenzen diskutiert vgl. www.wiwo.de/unternehmen/it/streit-um-it-sicherheit-nach-telekom-hackerangriff-der-fensterbauer-haftet-nicht-wenn-eingebrochen-wird/14914942.html, zuletzt geprüft am 03.12.2016. Es würde nicht verwundern, wenn bald auch in diesem Kontext die Forderung nach Verschärfung des Strafrechts erhoben werden würde, obwohl der Telekom-Fall gerade keine strafrechtliche Schutzlücke offenbart. Hier dürfte ziemlich sicher § 303b StGB erfüllt sein.

2

Vergütung für den anwaltlichen Zeugenbeistand im Strafverfahren

Leitsatz:

Einem Rechtsanwalt, der als Zeugenbeistand gemäß § 68b StPO für die Dauer der Vernehmung beigeordnet wird, steht grundsätzlich nur eine Gebühr wegen einer Einzeltätigkeit nach Nr. 4301 Nr. 4 RVG-VV zu.

Anmerkung zu OLG Braunschweig, Beschluss vom 26.09.2016, 1 Ws 145/16

von **Dr. Diana Hembach**, RA'in und FA'in für Strafrecht, Gercke & Wollschläger, Köln

A. Problemstellung

Der hier besprochene Beschluss des OLG Braunschweig befasst sich mit der Vergütung des anwaltlichen Zeugenbeistands. Das Gericht hatte über die Frage zu entscheiden, ob einem Rechtsanwalt, der als Zeugenbeistand gemäß § 68b StPO für die Dauer der Vernehmung beigeordnet wird, die Verteidigergebühr nach Nr. 4100 ff. VV RVG oder nur eine Gebühr wegen einer Einzeltätigkeit nach Nr. 4301 VV RVG zusteht.

B. Inhalt und Gegenstand der Entscheidung

Ein Rechtsanwalt, der als Zeugenbeistand gemäß § 68b StPO beigeordnet war, beantragte für seine Tätigkeit eine Vergütung in Höhe von etwa 3.000 Euro unter Zugrundlegung einer Grundgebühr gemäß Nr. 4101 VV RVG sowie einer Verfahrensgebühr gemäß Nr. 4119 VV RVG nebst Termingebühren und Längenzuschlag. Das LG Braunschweig setzte jedoch die zu erstattenden Gebühren mit Beschluss vom 10.02.2016 unter Zugrundelegung der Gebührentatbestände nach Nr. 4301 VV RVG und Nr. 4122 VV RVG auf 966,28 Euro fest.

Hiergegen erhob der Rechtsanwalt Erinnerung, die allerdings durch das LG Braunschweig zurückgewiesen wurde. Auch die Bezirksrevisorin des LG Braunschweig legte wegen eines Betrages in Höhe von 252,28 Euro Erinnerung ge-